



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,887	06/25/2003	Steven E. Campisi	DFC 03-1-2	4904
23531	7590	11/20/2008	EXAMINER	
SUITER SWANTZ PC LLO 14301 FNB PARKWAY SUITE 220 OMAHA, NE 68154			JOINSON, CARLTON	
ART UNIT	PAPER NUMBER			
		2436		
MAIL DATE	DELIVERY MODE			
11/20/2008	PAPER			

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/603,887	CAMPISI ET AL.
	<b>Examiner</b> CARLTON V. JOHNSON	<b>Art Unit</b> 2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### **Status**

1) Responsive to communication(s) filed on **14 August 2008**.  
 2a) This action is **FINAL**.      2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### **Disposition of Claims**

4) Claim(s) **55-76** is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) **55-76** is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### **Application Papers**

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### **Priority under 35 U.S.C. § 119**

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### **Attachment(s)**

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_  
 5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_

**DETAILED ACTION**

1. This action is responding to application amendments filed 6-25-2003.
2. Claims 55 - 76 are pending with Claims 1- 54 cancelled. Claim 55 is independent. Claim 55 has been amended. This application was filed 6-25-2003.

***Response to Remarks***

3. Applicant's arguments filed 8/14/2008 have been fully considered but they were not persuasive.

- 3.1 Applicant argues that the referenced prior art does not disclose, "the processor performing enrollment of said biometric feature of said user to produce said stored biometric data in said memory without employment of a device external to said housing, said stored biometric data remaining solely within said memory". (see Remarks Page 7); "an enrollment process". (see Remarks Page 7)

Shigematsu discloses enrollment of user information without usage of an external device. (see Shigematsu paragraph [0260], lines 1-5: fingerprint data of each user is registered in the fingerprint token of the user; when fingerprint data read by the sensor matches the registered fingerprint data; authentication output is generated and transmitted; paragraph [0260], lines 11-14: registered fingerprint data is not loaded in the machine such as a ATM; the user need not worry about misuse; paragraph [0261], lines 1-3: fingerprint data is registered in the storage unit of the authentication token) S discloses an authentication device within a single housing. (see Shigematsu Figure 2

(1a: main body section); paragraph [0067], lines 1-8: token indicates a compact and lightweight portable device used for authenticating a user; paragraph [0069], lines 1-4: main body section that includes the sensor, storage circuit, collation circuit, communications circuit, and connector)

3.2 Applicant argues that the referenced prior art does not disclose, "said stored biometric data remaining solely within said memory". (see Remarks Page 8)

Shigematsu discloses that the biometric data is stored within the token memory. (see Shigematsu paragraph [0260], lines 11-14: registered fingerprint data is not loaded in the machine such as a ATM; the user need not worry about misuse; paragraph [0261], lines 1-3: fingerprint data is registered in the storage unit of the authentication token)

3.3 Shigematsu discloses an authentication token card that authenticates a user without any additional equipment as per claim limitations. Biometric information is stored (registered) on the authentication token card. A biometric sensor is located upon the authentication token card to capture biometric information of current holder of authentication token card. The comparison of stored (registered) and current biometric information is done on the authentication token card. A wireless signal is output from the authentication token card after successful authentication. The wireless signal is a type of authentication OK signal to open an access gate or password or PIN to enable access to an automated teller machine. Additional dependent claim limitations further limit the claimed invention. (see Shigematsu paragraph [0012], lines 1-20:

authentication token card)

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 55 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant has amended claim 55 to include the limitation: "the processor performing enrollment of said biometric feature of said user to produce said stored biometric data in said memory without employment of a device external to said housing". The specification in paragraph [0013] (on page 7, lines 16-19) discloses: "The memory includes read only memory (ROM), such as electrically erasable programmable read only memory (EEPROM) or flash memory, to store card identification information for communications with external enrollment or access devices.". The specification discloses an external enrollment device. This is contrary to the amended claims limitation of "without employment of a device external to said housing". Also, the specification discloses that no external device is used for identity verification and not for enrollment as amended. (specification in paragraph [0008]; page

3, lines 16-18: "The present invention provides an identification card that **does not require external equipment for identity verification**, physical access control, logical access control, financial transaction authentication, and terminal login authentication.")

With the specification disclosing that enrollment and verification are separate steps.

Appropriate correction required.

***Claim Rejections – 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 55, 58, 60, 63, 67, 68, 69, 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shigematsu et al.** (US PGPUB No. 20020095588) in view of **Mosher** (US PGPUB No. 20030173408) and further in view of **Doyle et al.** (US PGPUB No. 20020095587).

**With Regards to Claim 55**, Shigematsu discloses a transaction authentication card, comprising:

a) a housing: (see Shigematsu Figure 2 (1a: main body section); paragraph [0067], lines 1-8: token indicates a compact and lightweight portable device used for authenticating a user; paragraph [0069], lines 1-4: main body section that includes the sensor, storage circuit, collation circuit, communications circuit, and

connector)

- b) a biometric sensor for sensing a biometric feature of a user, the biometric sensor disposed on said housing; (see Shigematsu Figure 2 and 2A (11: fingerprint sensor); paragraph [0012], lines 10-16: sensor for user biometric identification information; paragraph [0068], lines 1-2: biometric sensor is enclosed within the same housing for the authentication token)
- c) a memory disposed in said housing; (see Shigematsu Figure 1 (12: storage circuit): memory within housing for authentication token; paragraph [0161], lines 8-11: ROM; hard disk: a memory; memory is contained within the same housing as authentication token)
- f) a wireless transmitter capable of generating wireless signals, the wireless signal is transmitted on a one-to-one validation of the biometric feature (see Shigematsu paragraph [0012] lines 16-10: wireless communications used for communication of authentication data after biometric comparison (access control, financial transaction); col. 2, lines 61-65: different frequencies), the wireless signal being formatted as a human interface device signal (see Shigematsu paragraph [0202], lines 1-8; paragraph [0204], lines 1-8: data formatted for human interface device (a display); displays the door number received from the authentication token card), the transaction authentication card being operable with a financial transaction terminal or an automated teller machine terminal. (see Shigematsu paragraph [0250], lines 1-8: authentication token operates in financial transactions (using automated teller machine))

Shigematsu discloses wherein a processor (see Shigematsu paragraph [0161], lines 4-8: microprocessor for performing authentication functions) for retrieving stored biometric data representing a biometric feature of said user from the memory (see Shigematsu paragraph [0072], lines 1-5: storage of advanced registered data or biometric information for a user), the processor having a fingerprint matching algorithm for comparing a biometric feature of a user with the stored biometric data. (see Shigematsu paragraph [0012], lines 12-16: collation (comparison) of stored (registered) biometric information and current biometric information; results determine status of authentication) And, Shigematsu discloses wherein the processor being communicatively coupled to said biometric sensor and said memory and disposed in said housing, the processor performing enrollment of said biometric feature of said user to produce said stored biometric data in said memory without employment of a device external to said housing, said stored biometric data remaining solely within said memory (see Shigematsu paragraph [0260], lines 1-5: fingerprint data of each user is registered in the fingerprint token of the user; when fingerprint data read by the sensor matches the registered fingerprint data; authentication output is generated and transmitted; paragraph [0260], lines 11-14: registered fingerprint data is not loaded in the machine such as a ATM; the user need not worry about misuse; paragraph [0261], lines 1-3: fingerprint data is registered in the storage unit of the authentication token) Shigematsu does not specifically disclose the step of generating a serial number based on the biometric input.

However, Doyle discloses:

d) a serial number generation algorithm for generating a serial number based on the fingerprint matching algorithm; (see Doyle paragraph [0097], lines 1-5: identifier (i.e. serial number) generated for data processing)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby the step of generating a serial number based on the biometric input as taught by Doyle. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Shigematsu does not specifically disclose a system for erasing data.

However, Mosher discloses:

e) wherein a system for erasing data in said memory. (see Mosher paragraph [0070], lines 3-10; paragraph [0071], lines 8-17; paragraph [0098], lines 31-33: erasure capability for data)

The only disclosure within the specification of an erasure of data is when power source is shutdown. There is no disclosure within specification of an erasure of data via a command sequence or any other action.

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby a system for erasing data as taught by Mosher. One of ordinary skill in the art would have been motivated to employ the teachings of

Mosher in order to enable tamper detection, tamper prevention, secure transmission of information, and the integrity of the information, and the capability to prevent the unauthorized transfer of the information to others. (see Mosher paragraph [0006], lines 4-8: “*... wireless communications and data storage functions, opportunities for falsification and fraudulent use are increased. Of concern are insuring tamper detection, tamper prevention, secure transmission of information, the integrity of the information, and the prevention of unauthorized transfer of the information to others. Improvements in each of these areas are needed. ...*”)

**With Regards to Claim 58**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), wherein the wireless transmitter is an infrared transmitter. (see Shigematsu paragraph [0116], lines 1-7: infrared communications used in the place of radio communications between authentication token and use device)

**With Regards to Claim 60**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), further comprising a power supply. (see Shigematsu Figure 5 (BAT1; BAT2); paragraph [0118], lines 1-4; paragraph [0124], lines 1-4: battery, power supply)

**With Regards to Claim 63**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), wherein the wireless signal is encoded. (see Shigematsu paragraph [0246], lines 1-9: wireless communications; paragraph [0271], lines 1-5: communications between entities; wireless communications encrypted (encoded))

**With Regards to Claim 67**, Shigematsu discloses the transaction authentication card of Claim 55. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose that the antenna is a telescopic antenna. However, Doyle discloses wherein the antenna is a telescopic antenna. (see Doyle paragraph [0057], lines 7-15: antenna capability)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby the antenna is a telescopic antenna as taught by Doyle. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

**With Regards to Claim 68**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), wherein the memory stores multiple biometric data for a single user. (see Shigematsu paragraph [0012], lines 10-16: biometric data storage;

paragraph [0067], lines 5-8: multiple types of biometric data for a user) Shigematsu does not specifically disclose biometric data for multiple users. However, Doyle discloses wherein biometric data for multiple users. (see Doyle paragraph [0091], lines 6-10: biometric data for multiple users)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu for the storage of biometric data for multiple users as taught by Doyle. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

**With Regards to Claim 69**, Shigematsu discloses the transaction authentication card of Claim 55. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card; paragraph [0012], lines 10-16: biometric used for verification) Shigematsu does not specifically disclose providing more than one biometric for verification. However, Doyle discloses wherein providing more than one biometric for verification. (see Doyle paragraph [0035], lines 1-16: multiple types of biometric identification information processed for authentication)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu for more than one type of biometric for verification as taught by Doyle. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

**With Regards to Claim 71**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), wherein the card is used for access control, financial transactions, security transactions, government control, airline security, passport ID, and driver's license or authentication. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card; paragraph [0250], lines 1-8: financial transactions (automated teller machine); paragraph [0218], lines 1-4: access control)

6. Claims **56, 57, 59, 61, 62** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shigematsu-Mosher** and further in view of **Bashan et al.** (US Patent No. **6,202,927**).

**With Regards to Claim 56**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), where the wireless transmitter is a radio frequency transmitter and an antenna connection. (see Shigematsu Figure 6 (23; 42; COMMUNICATIONS DATA 4A); paragraph [0221], lines 1-7: radio frequency communications (wireless transmitter)) Shigematsu does not specifically disclose a loop antenna. However, Bashan discloses wherein further comprising a loop antenna. (see Bashan col. 6, lines 22-26: loop antenna)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu for a radio frequency transmitter and an antenna connection as taught by Bashan. One of ordinary skill in the art would have been motivated to employ the teachings of Bashan in order to enable the capability to use smart cards for process monitoring where relatively long range communication between the station and transponder is required in the order of several meters. (see Bashan col. 2, lines 9-18: “ *... Although smart cards are inherently well suited for portable, low-power applications, known smart cards suffer from low range communication, usually in the order of only 30 to 50 cm. This is acceptable for passive systems wherein a moveable transponder is brought into close proximity with a fixed station as is typically the case when data in the smart card is to be read by the station. However, it militates against the use of smart cards for process monitoring where relatively long range communication between the station and transponder is required in the order of several meters....* ” )

**With Regards to Claim 57**, Shigematsu discloses the transaction authentication card of Claim 56. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose a frequency of the radio frequency transmitter is between 1 KHz and 999 GHz. However, Bashan discloses wherein a frequency of the radio frequency transmitter is between 1 KHz and 999 GHz. (see Bashan col. 9, lines 66-67: radio transmission frequency (i.e. 13.56 MHz))

It would have been obvious to one of ordinary skill in the art to modify Shigematsu

for a radio frequency between 1 KHz and 999 GHz as taught by Bashan. One of ordinary skill in the art would have been motivated to employ the teachings of Bashan in order to enable the capability to use smart cards for process monitoring where relatively long range communication between the station and transponder is required in the order of several meters. (see Bashan col. 2, lines 9-18)

**With Regards to Claim 59**, Shigematsu discloses the transaction authentication card of Claim 55 further comprising a human interface device signal. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card; paragraph [0202], lines 1-8; paragraph [0204], lines 1-8: data formatted for human interface device (a display); displays the door number received from the authentication token card) Shigematsu does not specifically disclose where a device signal is compatible with Mifare. However, Bashan discloses wherein the device signal is compatible with Mifare. (see Bashan col. 9, lines 66-67: Mifare frequency (i.e. 13.56 MHz), wireless communications capability)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby a device signal is compatible with Mifare as taught by Bashan. One of ordinary skill in the art would have been motivated to employ the teachings of Bashan in order to enable the capability to use smart cards for process monitoring where relatively long range communication between the station and transponder is required in the order of several meters. (see Bashan col. 2, lines 9-18)

**With Regards to Claim 61**, Shigematsu discloses the transaction authentication card of Claim 60 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) with a power supply that is chargeable. (Shigematsu paragraph [0118], lines 1-4; paragraph [0118], lines 9-12: power (supply) may be supplied from a battery; secondary battery may be charged using power supply) Shigematsu does not specifically disclose that the power supply is rechargeable. However, Bashan discloses wherein the power supply is rechargeable. (see Bashan col. 3, lines 1-3: rechargeable power supply (i.e. battery))

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby the power supply is rechargeable as taught by Bashan. One of ordinary skill in the art would have been motivated to employ the teachings of Bashan in order to enable the capability to use smart cards for process monitoring where relatively long range communication between the station and transponder is required in the order of several meters. (see Bashan col. 2, lines 9-18)

**With Regards to Claim 62**, Shigematsu discloses the transaction authentication card of Claim 61 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card), wherein the power supply is a battery or capacitor. (see Shigematsu paragraph [0118], lines 1-4: power supply a battery)

7. Claims 64 - 66 are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Shigematsu-Mosher-Doyle** and further in view of **Elteto et al.** (US Patent No.

7,111,324).

**With Regards to Claim 64,** Shigematsu discloses the transaction authentication card of Claim 5. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose a multicolor light emitting diode. However, Elteto discloses wherein a multicolor light emitting diode. (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as status indication)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu to use multi-color light emitting diodes for a status indication as taught by Elteto. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62: “ ... From the foregoing, it can be seen that there is a need for a personal key that allows the user to store and retrieve passwords and digital certificates without requiring the use of vulnerable external interfaces. ... ”)

**With Regards to Claim 65,** Shigematsu discloses the transaction authentication card of Claim 64. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose a first color for a good read and a second color for a low battery. However, Elteto discloses wherein the multicolor light emitting diode indicates a first color for a good read and a second

color for a low battery. (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as a status (i.e. good read, low battery) indication)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu to indicate a first color for a good read and a second color for a low battery as taught by Elteto. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62)

**With Regards to Claim 66**, Shigematsu discloses the transaction authentication card of Claim 64. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose a third color for a state of enrollment. However, Elteto discloses wherein the multicolor light emitting diode indicates a third color for a state of enrollment. (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as a status (i.e. good read, low battery) indication)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby a third color for a state of enrollment as taught by Elteto. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62)

8. Claims 70, 72 - 75 are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Shigematsu-Mosher-Doyle** and further in view of **Jachimowicz et al.** (US Patent No. 5,734,154).

**With Regards to Claim 70**, Shigematsu discloses the transaction authentication card of Claim 55, wherein further comprising a processor. (see Shigematsu paragraph [0161], lines 4-8: microprocessor; paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose that the biometric sensor is on a front side of the card. However, Doyle discloses wherein a biometric sensor is on a front side of card.

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby a biometric sensor is on a front side of card as taught by Doyle. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Shigematsu-Doyle does not specifically disclose wherein an image is formed on a back side of the card. However, Jachimowicz discloses an image is formed on a back side of the card. (see Jachimowicz Figure 14; col. 1, lines 49-51: display for image viewing, image viewed through aperture)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu-Doyle whereby an image is formed on a back side of the card as taught by Jachimowicz. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for-viewing the

information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

**With Regards to Claim 72**, Shigematsu discloses the transaction authentication card of Claim 55. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose a display for showing an image downloaded by a user. However, Jachimowicz discloses wherein a display for showing an image downloaded by a user. (see Jachimowicz col. 1, lines 49-51: display for image viewing)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu for a display showing an image downloaded as taught by Jachimowicz. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

**With Regards to Claim 73**, Shigematsu discloses the transaction authentication card of Claim 72. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose that the image is a photo id. However, Jachimowicz discloses wherein the image is a photo id. (see Jachimowicz col. 1, lines 49-51: display for image (i.e. photo id) viewing)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu whereby the image is a photo id as taught by Jachimowicz. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to

provide an improved apparatus for viewing the information stored on a smart card.  
(see Jachimowicz col. 1, lines 34-37)

**With Regards to Claim 74**, Shigematsu discloses the transaction authentication card of Claim 72. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose that the displayed image is text. However, Jachimowicz discloses wherein the image is text.  
(see Jachimowicz Figure 14; col. 1, lines 49-51: display for image or text viewing)

It would have been obvious to one of ordinary skill in the art to modify Bashan whereby a display image is text as taught by Jachimowicz. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card.  
(see Jachimowicz col. 1, lines 34-37)

**With Regards to Claim 75**, Shigematsu discloses the transaction authentication card of Claim 55. (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) Shigematsu does not specifically disclose an alphanumeric keypad membrane for personal identification entry. However, Jachimowicz discloses wherein an alphanumeric keypad membrane for personal identification entry. (see Jachimowicz col. 3, lines 18-25: keypad membrane for data input)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu

for a keypad type data input capability as taught by Jachimowicz. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

9. Claim 76 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Shigematsu-Mosher-Doyle** and further in view of **O'Gorman** (US Patent No. 6,970,584).

**With Regards to Claim 76**, Shigematsu discloses the transaction authentication card of Claim 55 (see Shigematsu paragraph [0012], lines 1-20; paragraph [0078], lines 4-8: authentication token; data card) and a biometric sensor. (see Shigematsu paragraph [0138], lines 6-9: biometric sensor) Shigematsu does not specifically disclose a cover for access port. However, O'Gorman discloses wherein a cover for access port. (see O'Gorman col. 3, lines 6-9; col. 3, lines 26-28: biometric sensor cover)

It would have been obvious to one of ordinary skill in the art to modify Shigematsu for a cover over the access port as taught by O'Gorman. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27; col. 2, lines 4-7)

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information with regards to the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson  
Examiner  
Art Unit 2436

CVJ  
November 10, 2008